

## חלק תיאורתי:

### נימוח מצלות רשת ואבטחה:

**שאלה:** מכונת TEST EC2 לא הצליחה לקבל DNS resolve של כתובות אינטרנטיות, מה הן נקודות הcess אוון הייתה בוחן?

**תשובה:** קודם כל, אני מודאגת שהמכונה רשאית לבקש בבקשת DNS. זה נעשה באמצעות חוקים ב-Group Security ACL ו-Network ACLים שונים יוצאת בפורט 53, שהוא הפורט של DNS. לאחר מכן, אני בודקת שהמכונה יודעת למי לשלוח את בקשה DNS. AWS, זה בדרך כלל ה-VPC Resolver. אם הוא לא מוגדר נכון, הוא לא יודע להביא את התשובה מה האינטרנט.

**שאלה:** מכונת TEST EC2 מקבלת תרגום כתובות DNS אך נכשלת בתקשרות לאינטרנט (למשל, hub.docker.com ב-443), מה עשוי להיות מקור התקלה?

**תשובה:** אם DNS עובד, זה אומר שיש כתובות IP, אבל הנתונים לא מגיעים לייד. אני בודקת בטלית הנתוב של הרשות שהתנווה מכונת-LTGW ומשם לרכיב שיעוד ליצאת החוצה, זה NAT VPC EGRESS. בנוסף, ה-WF-NPF הוא חומר אש מרכזית. התנווה עובייה דרכו לפני שהיא מגיעה ל-NAT Gateway NAT ויצאת לאינטרנט. אם אין חוק שמאפשר EC2 לפנות החוצה בפורט 443, Firewall פשוט זורק את החיבור. בנוסף, גם אם כל הניתוב והWF-NPF תקין, Firewall ה-EC2 (Security Group) ח'יב לאשר את היציאה זו.

**שאלה:** על מכונת TEST EC2 מותקן docker engine, repo שלו נמצא ב-ALM Nexus במכונת-h-sus, מה הייתה בודק בינתן השגיאות הבאות:

### **שגיאה 1 : pull access denied**

**תשובה:** TEST EC2 הצליח להגיע ל-Nexus, אבל Nexus אמר לו "אין לך הרשות". אני בודקת אם החזון Logined בוצע נכון ואם משתמש יש הרשות מתאימות על ה-Repository.

### **שגיאה 2 : container pull time out**

**תשובה:** TEST EC2 ניסה לדבר עם Nexus אבל לא קיבל תגובה בכלל - הנתונים פשוט נעלמו. זה כמו תמיד חסימת רשות. אני בודקת אם TGW מנתב נכון, ואם חומר האש של Nexus (ה-Group Security) שלו מאפשר EC2 TEST לדבר אליו בפורט הנכון.

### **שגיאה 3 : docker daemon is not running**

**תשובה:** זו תקלה מקומית ל-Amazon. לפני שאני בודקת את הרשות או את Nexus, אני מודאגת שהמנוע (Docker Daemon) בטור EC2 בפועל, כי אם הוא כבוי, שום פקודה Docker לא תעבור.

**שאלה:** החצנת שירות אל מול האינטרנט מבוססת על רשומות DNS והפניה למכונת TEST EC2. בגישה מבחוץ מקבלים את הכתובת הציבורית של המכונה אך לא מצליחים לגלוש לשירות HTTPS, מה הייתה בודק בושם?

**תשובה:** Checkpoint FW הוא נקודת המעבר העיקרי לנכסים. אני בודקת בחוקי הפירול שלו האם הוא מאפשר חיבור HTTPS לעבר אל TEST EC2, אחריו שהחומר AISHER, החיבור מגיע ל-TEST EC2. עכשו אני בודקת שההדרת של EC2 (Security Group) פתוחה ל-443 לחיבורים שמגיעים מהחומר AISHER. אם הרשות והחוומות אשי תקין, הבעיה היא כנראה אחרת - אני בודקת שהאפקטיקציה בטור המכונה מוגדרת לטפל בחיבור HTTPS, HTTPS ושהתועודה (SSL Certificate) לא פגעה או לא מוגדרת נכון.

**שאלה:** בניסיון ביצוע telnet ממכונת TEST EC2 מתקבלת שגיאה שתוכנה זו חסורה, איך תתקן אותה על Linux 2 מה יכול להיות גורם לכשל ההתקינה שלו מה-Repo ובאיזה פקודה הייתה פותרת את זה?

תשובה: בנסען התקינה `telnetd` על 2 Amazon Linux, בדרך כלל נהוג להשתמש `telnetd`, אבל ההתקנה יכולה להיכשל אם השרת לא מצליח להציג YUM repositories של אמזון. זה קורה בדרך כלל בגלל בעיות תקשורת החוצה - למשל בעיות DNS, חסימה בSecurity Group או NACL, או מצב שבו השרת נמצא `private subnet` בלבד. בנוסף, לעיתים גם מטען פגום של yum גורם לתקלה. במקרה זה, הפתרון הוא לנוקוט את המטען NAT Gateway. בנוסף, לעיתים גם מבוקש כדי לבנות אותו מחדש, ולאחר מכן `makecache` ולחזור `clean all`.

#### הסבר שלי על התמונה:

שרת TEST EC2 מתחבר דרך NEXUS EC2 - Transit Gateway - שהוא הכלי המרכזי שאחראי לנtab את כל התעבורה בין רשתות ה-VPC השונות. לאחר מכן, כאשר מוכנת TEST EC2 רצה לצאת החוצה לאינטרנט (כמו בפורט 443), התעבורה נשלחת שוב TGW. TGW מנתב אותה ל-VPC INSPECTION - שם היא נבדקת על ידי חוממות אש מרכזיות (เช่น FW CHECKPOINT) המבצעות אבטחה וסינון של בקשות יציאה ונכנסות. לאחר מכן, התעבורה נשלחת ל-VPC EGRESS. EGRESS VPC מגדיר את חוקי התעבורה החוצה לאינטרנט. לבסוף, TGW מנתב את התעבורה המאפשרת אל NAT Gateway, ומשם היא יוצאת החוצה. NAT Gateway מאפשר לסדרנים פרטימ'ים לצאת לאינטרנט מוביל להיחשף לכנייה של בקשות ממנה, ובכך מספק שכבת הגנה נוספת.



